UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,637	10/12/2001	Verna E. Knapp	10018637 -1	3098

7590 05/02/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
OYEBISI, OJO O

ART UNIT	PAPER NUMBER
3692	

MAIL DATE	DELIVERY MODE
05/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/976,637	KNAPP ET AL.	
	Examiner	Art Unit	
	OJO O. OYEBISI	3692	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

In the amendment filed on 02/15/07, the following have occurred: claims 1-4, and 8 have been amended, claims 1-11 are pending, and claims 1-11 stand rejected in this office action. Further, the amendment has necessitated the withdrawal of 35 U.S.C. 112, second paragraph rejection.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

2. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krsul et al (Krsul hereinafter, US PAT: 5,839,119) in view of applicant's disclosed prior art (see the background of the invention, also see fig.1 of applicant's enclosed drawing).

Re claims 1. Krsul discloses a computer-readable medium having stored thereon a data structure comprising: information identifying a secret share of a finite set of secret

shares (i.e., Bank 18 makes an entry in this database for every buyer-seller pair with outstanding, valid electronic tokens. Bank 18 assigns a unique identifier, which we shall call a purse identifier, to the group of electronic tokens just generated. Banks 18 then notes the purse identifier in its database entry for this buyer-seller pair, as well as all of the session serial numbers of those electronic tokens. Bank 18 also stores the address of seller 17 in the database entry in case buyer 16 should wish to redeem unspent electronic token halves. That done, bank 18 advances to step 1026 from step 1025, see col.8 lines 17-45, specifically see col.8 lines 35-45, also see col.2 lines 19-48); and a secret share profile associated with the secret share and comprising a set of activities associated with the secret share, the set of activities corresponding to at least one activity conducted within a commerce system by at least a portion of a plurality of entities within a commerce system (i.e., the present invention result from splitting the electronic tokens in half using secret splitting. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending. Referring again to FIGS. 4A and 4B, for simplicity steps 1018-1024 show only one electronic token being split in half at a time; however, the present invention is consistent with

many electronic tokens being split at once. First, during step 1020, bank 18 selects one of the signed electronic tokens to be split using secret splitting, see col.7 lines 45-65, also see col.2 lines 19-48) (see the summary of the invention and the abstract), and wherein association of the activities with the plurality of secret shares facilitates anonymous transactions and anonymous recommendations (see col.6 lines 40-48), and wherein the past activities of the entity are kept private so that specific knowledge of the activities of the entity are unknown to third parties (i.e., anonymity, see col.6 lines 40-48). Krsul does not explicitly disclose at least one recommendation generated for a given entity associated with the secret shares based on the entity's past activities and an intersection of sets of activities associated with the entity's secret shares as an estimated activities list, and found in each set of activities associated with each secret share of the given entity's secret shares are included in the estimated activities list, wherein activities found in less than all of the sets of activities associated with the entity's secret shares are excluded; and recommendation accuracy controlled by modifying usage, number of activities and a size of a number of possible secret share sets for any given entity identity. However, the disclosed prior art discloses generating at least one recommendation for a given entity based on the entity's past activities and an intersection of sets of activities as an estimated activities list (i.e., Based on the knowledge of what products or services are being acquired, the provider 104 can often supply one or more recommendations to the entity. That is, if an entity purchases, for example, tickets to a classical music concert, the provider may be able to recommend other classical music concerts or even other products, such as recordings of classical

music. As providers become more familiar with additional specific activities performed by specific entities within the electronic commerce system (i.e., develop profiles about the entities), they can further refine their recommendations so as to provide more targeted or relevant recommendations with increased likelihood that the specific entities will follow up on the recommendations, see paras 0004 of the background of the invention); and recommendation accuracy controlled by modifying usage, number of activities for any given entity identity (i.e., As providers become more familiar with additional specific activities performed by specific entities within the electronic commerce system (i.e., develop profiles about the entities), they can further refine their recommendations so as to provide more targeted or relevant recommendations with increased likelihood that the specific entities will follow up on the recommendations. While specific knowledge of a given entity's on-line activities may be valuable to the provider as a source of providing recommendations, see paras 0004 of the background of the invention). Thus it would have been obvious to one of ordinary skill in the art to combine the secret splitting scheme disclosed by krsul with the old and well-known recommendation technique disclosed in the applicant's background of the invention and fig.1 to associate the recommendation with the secret shares of the entity, since Krsul already discloses secret shares via secret splitting, to provide security and low transaction overhead for both buyers and sellers, while still providing buyer anonymity.

Re claims 2. Claim 2 recites similar limitations to claim 1 and thus rejected using the same art and rationale in the rejection of claim 1.

Re claims 3 and 5. Krsul further discloses a method operating in a computer environment for a commerce system comprising a plurality of entities each having an associated entity identity that is stored as a plurality of secret shares amongst at least a portion of a plurality of shareholders (buyers and sellers) (i.e., Bank 18 makes an entry in this database for every buyer-seller pair with outstanding, valid electronic tokens. Bank 18 assigns a unique identifier, which we shall call a purse identifier, to the group of electronic tokens just generated. Banks 18 then notes the purse identifier in its database entry for this buyer-seller pair, as well as all of the session serial numbers of those electronic tokens. Bank 18 also stores the address of seller 17 in the database entry in case buyer 16 should wish to redeem unspent electronic token halves. That done, bank 18 advances to step 1026 from step 1025, see col.8 lines 17-45, specifically see col.8 lines 35-45, also see col.2 lines 19-48), wherein each plurality of secret shares comprises a subset of a finite set of secret share values (i.e. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces, see col.7 lines 45-55, also see col.2 lines 18-48), a method for estimating activities of a first entity of the plurality of entities, the method comprising: associating, for each entity of the plurality of entities, at least one activity conducted by the entity within the commerce system with each of the plurality of secret shares used to store the entity identity corresponding to the entity such that each secret share of the finite set of secret share values has associated therewith a set of activities from at least a portion of the plurality of entities; and generating, for the first entity, an estimated activities list comprising an intersection of sets of activities associated with each secret share of a first plurality of secret shares

used to store a first entity identity corresponding to the first entity (i.e., Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending. Referring again to FIGS. 4A and 4B, for simplicity steps 1018-1024 show only one electronic token being split in half at a time; however, the present invention is consistent with many electronic tokens being split at once. First, during step 1020, bank 18 selects one of the signed electronic tokens to be split using secret splitting, see col.7 lines 45-65, also see col.2 lines 18-48) (see the abstract and the summary of the invention), and wherein the past activities of the entity are kept private so that specific knowledge of the activities of the entity are unknown to third parties (i.e., anonymity, see col.6 lines 40-48). Krsul does not explicitly disclose generating a set of recommendations based on the estimated activities list and providing the set of recommendations to the first entity; and controlling recommendation accuracy by modifying usage, number of activities and a size of a number of possible secret share sets for any given entity identity. However, the disclosed prior art discloses generating a set of recommendations based on the estimated activities list and providing the set of recommendations to the first entity; and controlling recommendation accuracy by modifying usage, number of activities and a

size of a number of possible secret share sets for any given entity identity (i.e., Based on the knowledge of what products or services are being acquired, the provider 104 can often supply one or more recommendations to the entity. That is, if an entity purchases, for example, tickets to a classical music concert, the provider may be able to recommend other classical music concerts or even other products, such as recordings of classical music. As providers become more familiar with additional specific activities performed by specific entities within the electronic commerce system (i.e., develop profiles about the entities), they can further refine their recommendations so as to provide more targeted or relevant recommendations with increased likelihood that the specific entities will follow up on the recommendations, see paras 0004 of the background of the invention, also see fig.1 of applicant's drawings). Thus it would have been obvious to one of ordinary skill in the art to combine the secret splitting scheme disclosed by krsul with the old and well-known recommendation technique disclosed in the applicant's background of the invention and fig.1 (prior art) to provide security and low transaction overhead for both buyers and sellers, while still providing buyer anonymity.

Re claim 4. Claim 4 recites similar limitations to one of the limitations recited in claim 1 and thus rejected using the same art and rationale in the rejection of that limitation in claim 1.

Re claim 6. Krsul further discloses the method wherein generating the estimated activities list further comprises: retrieving, by an anonymity service provider in communication with the first entity and each of the first portion of the plurality of

shareholders (i.e., providing anonymity to buyer, and preventing sellers from building a dossier about the buyer, see col.6 lines 40-48), the plurality of profiles from the first portion of the plurality of shareholders; and calculating, by the anonymity service provider, the intersection by determining common activities that are found within each of the plurality of profiles (i.e., using its computer network bank 18 generates a first token half for the buyer. This is done by generating a random electronic string P whose bit length is equal to that of the selected signed token. The random string P is then used to create the second token half for the signed electronic token. Using its computer network, bank 18 generates the second electronic token half, Q, by performing a bitwise XOR of S.sub.BP (T) and P, resulting in Q. Neither the first electronic token half, P, nor the second electronic token half, Q, have any value of themselves; however, they can be combined together by a bitwise XOR to obtain S.sub.BP (T). This prevents seller 17 from redeeming tokens without the consent of buyer 16, as well as protecting seller 17 from double-spending by buyer 16. Note also, that buyer 16 can use her electronic tokens only for purchases with the selected seller. If she wishes to do business with another seller, she must obtain another, different set of token halves, col.8 lines 1-15).

Re claim 7. Krsul further discloses the method of claim 3, wherein the at least one activity includes purchase of at least one digital product (i.e., Note also, that buyer 16 can use her electronic tokens only for purchases with the selected seller. If she wishes to do business with another seller, she must obtain another; different set of token halves, col.8 lines 5-15).

Re claims 8-10. Krsul further discloses an apparatus for use in a commerce system comprising a plurality of entities each having an associated entity identity that is stored as a plurality of secret shares amongst at least a portion of a plurality of shareholders (i.e., the present invention result from splitting the electronic tokens in half using secret splitting. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending, see col.7 lines 45-65, see col.2 lines 18-48, also see **the abstract** for secret splitting of electronic token between buyers and sellers), wherein each plurality of secret shares comprises a subset of a finite set of secret share values (i.e. Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces, see col.7 lines 45-55, also see col.2 lines 18-48), the apparatus comprising: means for associating, for each entity of the plurality of entities, at least one activity conducted by the entity within the commerce system with each of the plurality of secret shares used to store the entity identity corresponding to the entity such that each secret share of the finite set of secret share values has associated therewith a set of activities from at least a portion of the plurality of entities; means for receiving sets of activities associated with each secret share of a first plurality of secret

shares used to store a first entity identity corresponding to a first entity; and means, coupled to the means for receiving, for generating an estimated activities list, for the first entity, comprising an intersection of the sets of activities (i.e., Secret splitting splits a secret, in this case the value of electronic token, into multiple pieces. None of the parties to the secret can learn the secret without all cooperating with one another to combine their secret pieces. Each secret piece is valueless on its own, as well as meaningless to anyone without all the other secret pieces. Because each electronic token half is valueless by itself, buyer 16 is protected from unauthorized redemptions of electronic tokens by seller 17. When session serial numbers are added to the electronic token halves, both bank 18 and buyer 17 are protected from double spending. Referring again to FIGS. 4A and 4B, for simplicity steps 1018-1024 show only one electronic token being split in half at a time; however, the present invention is consistent with many electronic tokens being split at once. First, during step 1020, bank 18 selects one of the signed electronic tokens to be split using secret splitting, see col.7 lines 45-65, also see col.2 lines 18-48) (see the abstract and the summary of the invention), **wherein past activities of the entity are kept private so that specific knowledge of the activities of the entity are unknown to third parties (i.e., anonymity, see col.6 lines 40-48)**. Krsul does not explicitly disclose means for generating a set of recommendations based on the estimated activities list, means coupled to the means for generating the set of recommendations, for providing the set of recommendations to the first entity, and means for controlling recommendation accuracy by modifying usage, number of activities and a size of a number of possible

secret share sets for any given entity identity. However, the disclosed prior art makes this disclosure (i.e., Based on the knowledge of what products or services are being acquired, the provider 104 can often supply one or more recommendations to the entity. That is, if an entity purchases, for example, tickets to a classical music concert, the provider may be able to recommend other classical music concerts or even other products, such as recordings of classical music. As providers become more familiar with additional specific activities performed by specific entities within the electronic commerce system (i.e., develop profiles about the entities), they can further refine their recommendations so as to provide more targeted or relevant recommendations with increased likelihood that the specific entities will follow up on the recommendations, see paras 0004 of the background of the invention). Thus it would have been obvious to one of ordinary skill in the art to combine the secret splitting scheme disclosed by krsul with the old and well-known recommendation technique disclosed in the applicant's background of the invention and fig.1 to associate the recommendation with the secret shares of the entity, since Krsul already discloses secret shares via secret splitting, to provide security and low transaction overhead for both buyers and sellers, while still providing buyer anonymity.

Re claim 11: Claim 11 recites similar limitations to claim 6 and thus rejected using the same art and rationale in the rejection of claim 6.

Response to Arguments

3. The applicant has amendment the claims to include a new limitation: "wherein the past-activities of the entity are kept private so that specific knowledge of the activities of the entity are unknown to third parties." The newly added limitation is basically describing anonymity – i.e., "wherein the past activities of the entity are kept private..." Thus, the prior art of record, Krsul meets the newly added limitation in the following ways: Buyer 16 takes the signed and sealed first electronic message and attaches it, or appends it to, a second electronic message directed to the selected seller 17. Buyer 16 indicates her bank and its address, to which the enclosed, signed, and sealed electronic message should be forwarded. Note that the message need not indicate the buyer's identity to seller 17, providing anonymity to buyer 16, and preventing sellers from building a dossier about buyer 16. When the second electronic message is complete, buyer 16 transmits it to the selected seller 17. Now, buyer 16 awaits receipt of electronic token halves, see col.6 lines 40-48. It is clear from Krsul disclosure supra that buyer's anonymity is guaranteed, and as a result specific knowledge of the buyer's activities is not divulged to third parties.

The applicant further argues that the applicant background of the invention discussed the problems and the shortcomings of the prior systems, so for the examiner to use this against the applicant would amount to impermissible hindsight. In response to Applicant's argument that the Examiner's conclusion of obviousness is based upon

improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. *In re McLaughlin, 443* F.2d 1392; 170 USPQ 209 (CCPA 1971). The examiner maintains that the disclosed prior art in the applicant's background of the invention teaches and meets some of the limitations claimed by the applicant. Although, it is mentioned that the disclosed prior art is deficient i.e., While specific knowledge of a given entity's on-line activities may be valuable to the provider as a source of providing recommendations, which recommendation may even be helpful to or welcomed by some of the targeted entities, an increasing number of consumers object to commercial enterprises and other third parties having specific knowledge of their on-line activities. Clearly, a consumer's desire for privacy conflicts with the desire of commercial enterprises' to be able to recommend additional services and products based on past activities by consumers. **Therefore, a need exists for techniques that allow the formulation of recommendations based on some degree of knowledge about a given entity's on-line activities, but that also provides the given entity with a corresponding degree of privacy, see paras 0004-0005).** However, the primary reference, Krsul cures the deficiency of the disclosed prior art by using the secret splitting scheme taught by Krsul to guarantee anonymity to the consumers and by so doing, provides a certain degree of privacy to the consumers. Thus it would have been obvious to one of ordinary skill in the art to combine the secret

splitting scheme disclosed by krsul with the old and well-known recommendation technique disclosed in the applicant's background of the invention and fig.1 (prior art) to provide security and low transaction overhead for both buyers and sellers, while still providing buyer anonymity.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OJO O. OYEBISI whose telephone number is (571) 272-8298. The examiner can normally be reached on 8:30A.M-5:30P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, RICHARD E. CHILCOT can be reached on (571)272-6777. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

***

RICHARD E. CHILCOT, JR.
SUPERVISORY PATENT EXAMINER